TÜRK BİLİM ARAŞTIRMA VAKFI
TÜBAV
1995
TURKISH SCIENCE-RESEARCH FOUNDATION
TUBAV BILIM DERGISI

Yıl: 2009, Cilt:2, Sayı:2, Sayfa:138-147

MOBİL ORTAMLARA YAPILAN SALDIRILAR ÜZERİNE BİR İNCELEME

Şeref SAĞIROĞLU*, Murad A. MOHAMMMED

Gazi Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, Maltepe, 06570, Ankara

Özet

Günümüzde yaşantımızın vazgeçilmezleri arasında yer alan mobil teknolojiler, iletişim hizmetinin yanında insan hayatını kolaylaştıracak birçok yenilik sunmaktadır. Bu ortamlarda en çok kullanılan cep telefonları ise hafifliği ve küçülen boyutları bunu yanında sunduğu pek çok önemli hizmetler ile insan yaşantısındaki yerini her geçen gün daha fazla sağlamlaştırmaktadır. Bu ortamların kullanımının yaygınlaşması ile de bu ortamlara güven ve bu ortamlardaki güvenlik daha çok sorgulanmaya başlamaktadır.

Bu çalışmada mobil ortamlarda meydana gelebilecek güvenlik açıkları incelenmiş, literatürdeki mevcut çalışmalar gözden geçirilerek karşılaşılacak durumlar genel olarak değerlendirilmiş ve çözüm önerileri sunulmuştur.

Anahtar Kelimeler: Mobil ortamlar, saldırılar, açıklar, inceleme

A SURVEY ABOUT MOBILE ENVIRONMENT ATTACKS

Abstract

The mobiles technologies have been very efficient in the daily life and have started to provide many facilities to our life in many places, passing beyond the communication aim. Mobile phones mostly prefered devices in that environment have been the integral part of us, being lightweight and small size as well as the features such as many fascinating support. As a result, widespread usage of mobile electronic media have been increased. For these reasons, security in and trust to mobile systems have been questioned more and more.

In this study, vulnerabilities encountered in mobile electronic media have been revised and the studies in the literature were reviewed, the type of attacks were summarised, the work was finally concluded.

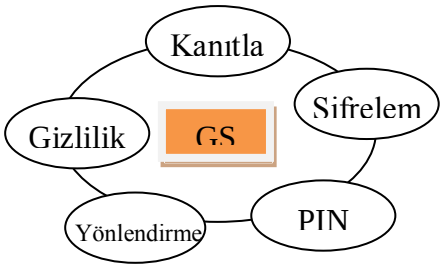
Key Words: Mobile environment, vulnerabilities, attacks, review

* E-posta: ss@gazi.edu.tr

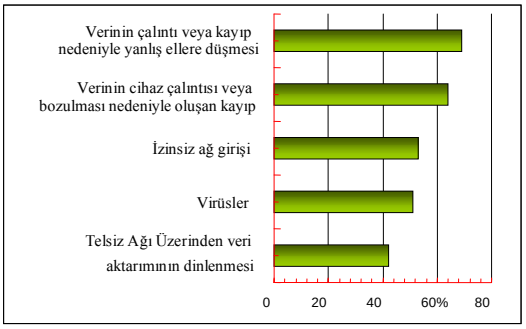
1. Giriş

GSM[2] ağlarındaki abone kimlik modülünün (SIM[3]) görevi, sadece yetkili kullanıcıların ağa erişebilmelerini sağlamaktır. Bir kullanıcıyı tam olarak onaylamak için ağ, veriyi depolayabilmeli, depolanmış veriye yetki dışı erişimden koruyabilmeli ve güvenlik şartları altında şifreli haberleşmeyi destekleyebilmelidir. SIM, mobil cihaz ve altyapı şebeke sistemleri ve hizmetleri ile kullanıcıların güvenli haberleşmesi sağlanmaya çalışılır. GSM ağlarında temel güvenlik bileşenleri, Şekil 1'de verilmiştir [1]. Şekilde verildiği gibi GSM ortamında güvenlik, şifreleme, PIN, yönlendirme, gizlilik ve kimlik doğrulama (kanıtlama) bileşenleri ile yapılmaktadır.

Mobil şebekelerin (SIM kart, cihaz, altyapı donanımı) hangi açıklardan daha çok etkilendiğine dair yağılan bir araştırma sonucu Şekil 2'de verilmiştir. Şekil 2'den de görülebileceği gibi en fazla kayıp çalıntı veya unutkanlıklardan kısaca insan zafiyetlerinden kaynaklanmaktadır.



Şekil 1. GSM güvenlik bileşenleri



Şekil 2. Mobil cihazları ve kullanıcıları [2]

Bu saldırıların nasıl gerçekleştirildiğini ve mobil ortam güvenlik seviyesinin ne kadar ihlal edildiğini anlamak için önce GSM ağlarında sağlanan güvenliği gözden geçirmekte fayda vardır. [22] ve [23] nolu kaynaklarda açıklandığı gibi GSM güvenlik prensipleri aşağıda sıralanmıştır.

- Kullanıcı kimliğininin gizlenmesi,
- Kullanıcı kimliğinin yetkilendirilmesi/doğrulanması,
- Kullanıcı trafiğinin ve kullanıcı ile ilgili kontrol bilgilerinin şifrelenmesi ve
- SIM'in güvenlik modülü olarak kullanımıdır.

Burada; *Kullanıcı kimliğininin gizlenmesi* ile havadaki mobil trafikten faydalanan kullanıcının güvenli olarak iletişimini sürdürmesi ve saldırganlardan korunması için gereklidir. *Kullanıcı kimliğinin yetkilendirilmesi* ile mobil operatörün doğru kullanıcıyı belirlemesi sağlanır. *Kullanıcı trafiğinin ve kullanıcı ile ilgili kontrol bilgilerinin şifrelenmesi* ile havadan yapılabilecek saldırılara karşı hassas bilgiler korunabilmektedir. *SIM'in güvenlik modülü* ile hem kullanıcının hemde operatörün güvenli iletişim yapmasını ve haberleşmeyi sağlıklı olarak yürütebilmek amacıyla anahtar dağıtımı, yetkilendirme ve anahtar üretimi için kullanılmaktadır. GSM ağları üzerinde SIM onaylama prosedürü, abonenin SIM kartının geçerliliğini kontrol eder ve ardından mobil istasyona özel bir ağ

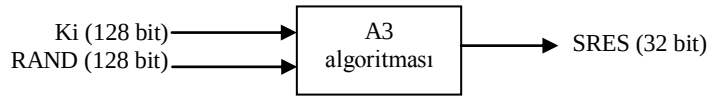
[2] Küresel Mobil İletişim Sistemi
[3] Abone Kimlik Modülü

üzerinde onay verilip verilmediğini denetlenir. Onaylama sürecine katılan taraflar, gri listede olmayan ve onaylı el cihazı olan SIM kartın son kullanıcısı veya sahibi ve ağ operatörüdür [3]. GSM şebekelerinde güvenliğin sağlanması için bazı algoritmalar kullanılmaktadır. Bu algoritmalar Bölüm 2'de açıklanmıştır.

2. GSM güvenlik algoritmaları

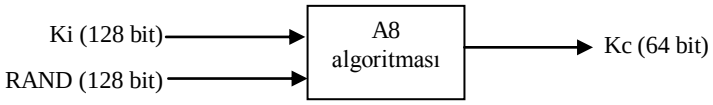
GSM şebekelerinde güvenlik genellikle üç algoritma desteğiyle sağlanmaktadır. Bu algoritmalar, Mobil İstasyonu Doğrulama Algoritması, Anahtar Üretme Algoritması ve Şifreleme Algoritması olarak sıralanabilir [3-5,10].

Mobil İstasyonu Doğrulama Algoritması: Kimlik doğrulama işinden sorumlu olan bu algoritma A3 olarak bilinir [3]. İlk olarak A3 algoritması 128 bit uzunluğundaki RAND[4] sayıyı BS[5]'den ve 128 bit uzunluğundaki kullanıcı kimlik doğrulama anahtarı Ki'yi SIM'den girdi olarak alır (Şekil 3). Daha sonra 32 bit uzunluğundaki SRES[6] çıktısını oluşturur. Bu 32 bitlik SRES, GSM ağındaki SRES ile karşılaştırılır. Eğer birbirleriyle uyuşuyorsa kimlik doğrulanır. A3 algoritması tek yönlü özetleme fonksiyonu kullanır, dolayısıyla ele geçirilen bir SRES'den Ki[7]'nin bulunması çok zordur [4].



Şekil 3. A3 Algoritması

Anahtar Üretme Algoritması: A8 algoritması bunlardan biridir [5]. Ses verisini şifrelemekte kullanılacak anahtarı üretme algoritmasıdır. A8, gizli anahtar Ki'yi ve MSC'den RAND'ı alarak oturum anahtarı Kc[8]'yi üretir (Şekil 4). İlk olarak A8 algoritması, 128 bitlik RAND ve 128 bitlik Ki'yi girdi olarak alır. Bunları kullanarak, 64 bitlik şifreleme anahtarı Kc'yi çıktı olarak verir. Kc, MSC tarafından MS[9]'nin doğruluğu tekrar onaylanmaya karar verilene kadar kullanılır. Bu bazen birkaç gün alabilir. A3 ve A8 algoritmalarının ikisi de tek yönlü fonksiyonlardır [5].

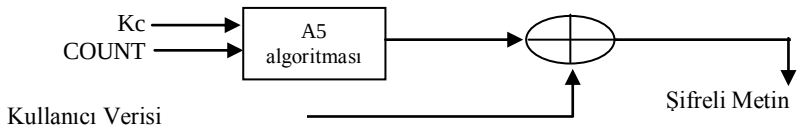


Şekil 4. A8 Anahtar Üretme Algoritması

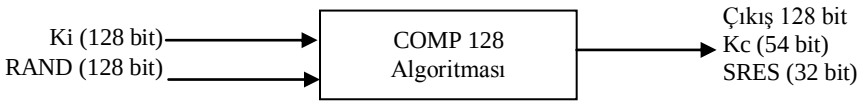
Şifreleme Algoritması: A5, bu algoritmalardan birisidir ve hava kanalı üzerinden şifreli veri gönderiminde kullanılır. A5 algoritmasının A5/1, A5/2 ve A5/3 gibi çeşitli varyasyonları vardır [3]. A5/1 hava kanalı üzerinden ses şifrelemesinde kullanılan güçlü şifreleme algoritmalarından biridir. Ancak A5/2 gibi başka sürümleri de Avrupa dışında kullanılmaktadır. Üçüncü nesil cep telefonları içinse A5/3 tasarlanmıştır. A5 ilk olarak A8 tarafından üretilen 64 bitlik şifreleme anahtarı Kc ile her çerçevenin numarasını (frame number) girdi olarak alır ve 228 bitlik anahtar akım dizisi oluşturur. Bu 228 bitin 114'ü MS'den BS'e gönderilen verilerin şifrelenmesinde diğer 114 bitlik blok ise BS'den MS'e gönderilen verilerin şifrelenmesinde kullanılır (Şekil 5). A5, A3 ve A8'in aksine SIM kart yerine cep telefonunun kendisinde çalışır. A5 algoritması şifreleme için dizi şifreleme (stream cipher) mekanizmasını kullanır. Veri, hava ortamıyla Kc kullanılarak şifrelenmiş çerçeveler (frame) olarak gönderilir.

COMP128 Algoritması: Dünyanın hemen hemen her yerinde GSM operatörleri, A3 ve A8 algoritması birlikte gerçekleştiren COMP128 algoritmasını kullanmaktadır [5]. COMP128 algoritması, RAND'i BS'den ve Ki'yi SIM'den alır. Fakat A3 ve A8'in aksine çıktı olarak 128 bit üretir. Bunun ilk 32 biti SRES olup, son 54 bitinin sonuna 10 tane sıfır ekleyerek ise Kc'yi üretir (Şekil 6).

[4] Rasgele Sayı
[5] Baz İstasyonu
[6] İşaretlenmiş Karşılık
[7] Kullanıcı Kimlik Doğrulama anahtarı
[8] Oturum Anahtarı
[9] Mobil İstasyon



Şekil 5. A5 algoritması



Şekil 6. COMP128 algoritması

GSM şebekelerinde güvenlik, yukarıda kısaca özetlenen algoritmalar ile bu algoritmaların şebeke içerisinde haberleşmesi prensibine dayanmaktadır [7].

3. Mobil ortam saldırıları

Mobil ortamların taşıdığı önemle birlikte bu ortamlara karşı yapılan saldırılarda artışlar olmuştur. Bu saldırılar: SIM kartları saldırıları, baz istasyonları, kablolu hattan gelen tehditler, kablosuza özgü tehditler, SMS[10] sazan avlama tehditleri, mobil ortam virüsleri ve solucan tehditleri, kontrol edilmemiş mobil mesajlaşma suiistimali, frekans taramalı sistemler, kullanıcının bloke edilmesi ve ara bağlamı ortamında yapılan saldırılar olarak sınıflandırılabilen bu saldırılar aşağıda takipeden alt başlıklarda özetlenmiştir [4,7,8,12,19].

3.1. SIM kartları

SIM kartlar, gizli anahtar Ki'yi içinde barındıklarından çok önemlidirler. Bu anahtar, hem kimlik doğrulama (authentication) hem de oturum anahtarı Kc'nin oluşturulmasında kullanılmaktadır. Bu yüzden Ki hiçbir şekilde havadan gönderilmez, yalnızca iki yerde saklı tutulur. Bunlar kullanıcı SIM kartı ve GSM ağ birimi HLR'dir. Aslında A3 ve A8 algoritmalarının SIM kartının içerisinde bulunmasının bir nedeni de Ki bilgisinin SIM kart dışına çıkmasının engellenmesidir. Bu yüzden, eğer Ki saldırgan tarafından ele geçirilirse, sadece konuşmaları dinlemekle kalmaz, SIM kartı sahibi abonenin hesabına yanlış faturalar yerleştirebilir. Mevcut aboneyi, Ki'yi kullanarak taklit edebilir. GSM sisteminin, bu durum için kısmi bir önlemi vardır. Aynı ID'li (kimlik numaralı) iki telefon aynı anda açıldığında, GSM ağı bunu fark ederek telefonlar için yer belirleme sorgusu yapar ve aynı kullanıcı numarasının aynı zamanda iki farklı yerde bulunduğunun farkına varırsa saldırganın ve meşru abonenin arama yapmasını engellemektedir. Ne var ki, saldırgan yalnızca kullanıcının konuşmalarını dinlemek isterse bu bir çözüm olmayacaktır. Bunun sebebi, saldırganın pasif olarak kalıp sadece konuşmaları dinleyerek GSM sisteminin kendisini tespit etmesini engellemesidir.

Son yıllarda yayımlanan bir raporda [12x], SIM kartlar üzerine optik hata induksiyonu yapan yeni bir saldırı türünü bildirmiştir. Bunun da geliştirilen bir teknikle smartkart işlemcisinin işlemlerinin bir elektronik kamera flaşıyla durdurulabileceğini belirtmişlerdir.

3.2. Sahte baz istasyonları

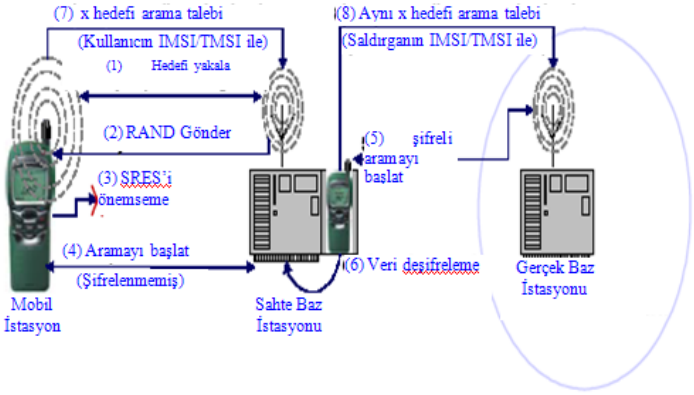
Sahte baz istasyonları, herhangi bir operatörün faaliyet gösterdiği frekanslarda daha fazla güç vererek o operatöre ait kullanıcıların kendisine bağlanmasını sağlamaktadır. Böyle bir durumda kullanıcı kendisini normal olarak GSM ağına bağlandığını düşünmekte ve bütün veri aktarımını bu baz istasyonu üzerinden yapmaktadır. Kullanıcının böyle

[10] Kısa Mesaj Hizmeti

bir durumu fark edememesinin sebebi, GSM de kimlik doğrulamanın tek yönlü olarak yapılmasıdır. Yani ağ kullanıcıyı kabul etmek için kimlik doğrulama işlemine tabi tutarken, kullanıcı karşısındaki GSM ağının doğru olup olmadığını test edemez. Şekil 8'de sahte baz istasyonu saldırılarının adımları verilmiştir. Şekil 8'de sahte bir baz istasyonuna bağlanmış kullanıcıya, sahte baz istasyonu sürekli olarak RAND gönderip ona karşılık gelen SRES'leri alabilir. SIM kartları bölümde bahsedilen metotla elde edilen SRES'lerden kullanıcının Ki'si elde edilebilinir. Bu saldırıyı gerçekleştirmek yaklaşık olarak 8-13 saate ihtiyaç vardır. Eğer kullanıcı sürekli olarak RAND bombardımanına tutulursa, telefon şarjı daha çabuk biteceğinden, kullanıcı durumdan şüphelenebilir. Dolayısıyla, saldırı çeşitli zaman dilimlerinde yapılarak da gerçekleştirilebilir [7].

3.3. Kablolu hattan gelen tehtidler

Teknoloji uyumu, e-posta, Web, SMS ile WAP[11] gibi telsiz servisleri biçimindeki geleneksel kablolu hat servislerine köprü kuran cihazların ve servislerin maliyetini düşürmede yardımcı olmaktadır. Cep telefonundan gönderilen SMS'in oldukça yüksek maliyeti gibi ekonomik bariyerler, kablosuz boşluğun kablolu ağlar ile görülen mesajlaşmanın kötüye kullanımını kolaylaştırmaktadır. Ancak bu bariyer, iki teknoloji arasındaki gittikçe artan kesintisiz ara birimle hafifletilmektedir. E-postadan SMS'ye olan ağ geçitleri, herhangi bir e-posta kullanıcısının dünyanın dört bir yanındaki mobil abonelerine ücretsiz mesajlar göndermesine olanak sağlamaktadırlar. İstenmeyen e-posta göndericileri (spammer) SMS/metin mesajları göndermek için cezalandırılmadıklarından dolayı bu aynı zamanda, mobil kullanıcılar içinde bir sorun olmaktadır. E-postadan SMS atma hizmeti, abonelerin arkadaşlara ve kullanıcı gruplarının sayfasına ulaşmak için kullandıkları popüler bir servistir, bu nedenle bu servisin kesilmesi veya kısıtlanması çokta iyi olmayacaktır. Ayrıca, mobil operatörleri aynı tip filtrelerle e-postadan SMS'e geçişler için kendi e-postalarını ve geniş İSS'lerin kendi e-posta altyapısını kapsaması için kullandığı içerik analiz sistemlerini korumalıdırlar. Mobil ortam müşterileri, sadece internet üzerinden halen mevcut daha fazla özellik talep ettikleri için mobil mesaj iletişiminin kötüye kullanımını çokta sınırlanamamaktadır. Konuları daha karmaşık hale getirmek için e-posta ve diğer iletişim formları cep telefonlarının ve PDA[12]'ların ötesine geçerek yeni cihaz kategorilerine uzanmaktadır. Televizyon set üstü kutularından buzdolaplarına kadar değişen aralıkta internete bağlı cihazlar mesaj gönderebilen platformların desteğiyle hızla yayılmaktadır. Oyun konsollarının ve portatif eğlence cihazlarının son dalgası da bu cihazların kullanıcılarının büyük çoğunluğu olan küçüklere ulaşan uygun olmayan içerik hakkında ek endişeler ortaya çıkaran İnternet bağlantısı ve mesajlaşma kapasitesine sahiptir. Bu platformlarda suistimal olayı hala bilinmezken kullanıcıların bilgisiyle birlikte mevcut cihaz sayısının fazlalığı, bu platformları saldırganlar ve suistimal ediciler için zorunlu hedefler haline getirmektedir [8].



Şekil 8. Sahte baz istasyonu saldırısı [7]

3.4. Kablosuza özgü tehditler

Kablosuza özgü mesajlaşma tehditleri, kablolu alandakilere benzemektedir fakat özel faktörlere bağlı olarak değişkenlik göstermektedir. SMS gönderme maliyetinin yaklaşık bir peni olduğu Japonya ve Güney Kore'de mobil spam oranı neredeyse e-posta spam'ı ile birlikte eşit durumdadır. Japonya'nın NTT DoCoMo ağında 10 mesajdan 9'u spam'dır. Güney Kore'de aboneler, cep telefonlarına her gün ortalama bir spam almaktadırlar. SMS

[11] Kablosuz Uygulama Protokolü
[12] Cep Bilgisayarı

göndermeyle bütünleşen her mesajın maliyeti ABD ve Avrupa'dakine denk gelinceye kadar buradaki kullanıcılar, kablolu ağlarda hâkim olan URL'lerin ve geniş yayın postalarının yerine muhtemelen kısa kodlar ve dar bir şekilde hedeflenmiş duyurular görecektir. Örneğin bir kullanıcı, mobil operatörün ücretlendirme sistemine bağlı kısa bir kod kullanan metin servisi için kendisinin bağlanmasını teşvik eden bir spam alabilir ya da özel bir ücret rakamıyla arama için aldatılabilir. Özel ücretli telefon numaralarının oluşumundaki kolaylık bu tür aldatmacayı özellikle dolandırma benzeri saldırıların önünü açabilir. Bu "yanlış ön metin" mesajları, daha fazla müşteri memnuniyetsizliğine yol açarak aboneler üzerinde doğrudan ve ani mali etkiye sahip olabilmektedir [8].

3.5. SMS sazan avlama (smishing) tehditleri

Mobil bankacılık ve mobil ödemenin on milyonlarca abone katılımıyla Japonya ve Güney Kore'de son derece popüler olduğu görülmüştür [19]. Bankalar tarafından düşük maliyetle bankacılık hizmetleri vermenin bir yolu olarak kabul edildiğinden banka memurlarından cep telefonuna doğru bir dönüş vardır. ABD'deki 1 numaralı mobil operatörü olan Cingular Wireless, müşterilerinin cep telefonlarından hesaplarını yönetmelerine olanak sağlayan mobil bankacılık hizmetini 2007 yılından itibaren sunmaya başlamışlardır. Dünyadaki mali kurumlar, SMS üzerinden hesaba erişim gibi SMS hizmetleri sunmaktadırlar ve SMS, işlemler veya hesaptan çekilen fazla paralar gibi yapılan hesap faaliyetleri konusunda müşterileri uyarır. Banka ile mobil müşteri arasındaki bu yeni doğrudan etkileşim, sazan avlama saldırısı yapanlar için kimlik hırsızlığı ve diğer sahtekârlık türleri amacıyla mobil kullanıcılardan mali bilgileri elde etme yönünde saldırganların iştahlarını arttırmaktadır. Bazı saldırılarda kullanıcıların, virüsü kendi el cihazlarına kabul etmeleri ya da kredi kartı numaraları ve diğer özel bilgileri vermeleri için girişimlerde bulunduktan sonra - alıcıların bir servise kaydolmalarını ister. Kontörlü cep telefonlarının kullanıcılarına karşı SMS sazan avlama saldırısı bildirimleri de alıcıların cep telefonlarına kontörlerini tekrar yüklemeleri için hesap bilgilerini girmelerini istemektedir. Geniş ölçekli SMS sazan avlama saldırısı veya "smishing" muhtemelen birçok büyük banka bu hizmetleri sunduktan ve yeterli sayıda kullanıcı kabul ettikten sonra kısa bir süreye kadar ortaya çıkmayacaktır. Ara dönemde bu saldırılar eğlence amaçlı olacaktır. Azalan saldırı hacmi, hacim tabanlı içerik bloke edilmeye bağlı olmayan çözümler gerektirmektedir. Fakat bunun yerine hem bal çanağılar ve diğer sensör ağları üzerinden algılanan saldırıları öncellikli olarak hem de kullanıcıya destek sağlamak için hızlı bir şekilde tepki gösterebilir [8].

3.6. Mobil ortam virüsleri ve solucan tehditleri

Günümüzde 130'da fazla 3G şebekesi bulunduğu ve bunların 1.4 Mbps ile 128 Kbps indirme ve yükleme hızlarında destek verdiği bilinmektedir [20]. Bu hızların 2008'de 7.3 Mbps ve 2009'da 10.2 Mbps'ye ulaşması beklenmektedir [21]. Bu yaygınlaşma beraberinde de bu ortamlardaki virüs ve solucanların daha da yaygınlaşmasını kolaylaştırmaktadır. Kötü niyetli yazılımların ortaya çıkışını mobil ortamlarda kullanılan yazılım ve platformların standartlaşması da arttırmıştır. Windows Mobil veya Symbian gibi işletim sistemleri olan mobil cihazların kullanımı artarken, mobil virüslerde de arttışlar kaçınılmazdır [12].

3.7. Kontrol edilmemiş mobil mesajlaşma suistimalinin etkisi

Spam e-postada kullanıcıları kızdırırken mobil cihazlarda izinsiz giren ve maliyetli olan bir şeydir. Bir SMS mesajı, aboneyi yüksek maliyetler kaybına uğratabilir. Ayrıca ön ödemeli hatlardaki dolandırma veya reklam mesajları birçok defa genel SMS gönderme/alma maliyetlerinden çok daha büyük mali etkiye sahip olabilir. Bu nedenle mobil spam müşterinin şikayetlere kaydolmasını veya kontör istemesini destekleyecek aramaları tetikleyecektir. Mobil sazan avlama saldırısı, aboneyle mali grup arasındaki ilişkiyi felce uğratarak abone için çok daha ciddi mali ve özel etkilere sahip olur. Mobile spam, abone ile servis sağlayıcısı arasındaki güven bağını da bozabilir. Bu kaybolan güven, abonelerin operatörden ve ortaklarından gelen yasal mobil reklamı kabul etmelerini zorlaştıracaktır. Son olarak kontrol edilmemiş SMS spam akışı, mobil operatörün servis kalitesi üzerinde ciddi sonuçlar doğurabilir. SMS mesajları, sesli aramalar olarak aynı kanal üzerinden aktarılmaktadır, böylece büyük hacimli SMS spam'ı ağa aşırı yükleme yapıp sesli hizmetlerin kabul edilmemesine yol açar. Bazı gelecek nesil SMSC'ler SMS ağı üzerinden sınırlı-ücretli trafik kapasitesine sahip olurken durum genellikle ekipmanı kurulu değildir. Ayrıca dış kaynaklı MT-SMS[13] trafiği doğrudan abone MSC'lerine gönderildiğinden harici ağlardan gelen trafiğin kabul oranı üzerinde genellikle çok az kontrol bulunmaktadır [8].

[13] Mobilde sonlanan - Kısa Mesaj Hizmeti

3.8. Frekans taramalı sistemler

Saldırganlar, kullanıcı ile baz istasyonu arasındaki trafiği frekans tarayıcılar ile analiz edilebilmektedirler. Önce bahsedildiği gibi alınan bilgi A5 algoritmasında Kc anahtarıyla şifrelenen metindir. Ancak, saldırgan A5 algoritmasındaki farklı zafiyetlerden yararlanarak şifre çözümünün süresini daha kısa sürelere indirebilir. Frekans tarayıcılı sistemler aracılığıyla yapılan saldırılarda karşılaşılabilecek en büyük problemi GSM operatörü tarafından yapılan frekans atlamasıdır (frequency hopping). Bu çözüme rağmen saldırganlar, kullanıcının IMSI[14]'sini yalnızca belirli zamanlarda göndermesinden dolayı yakalayabilirler [4].

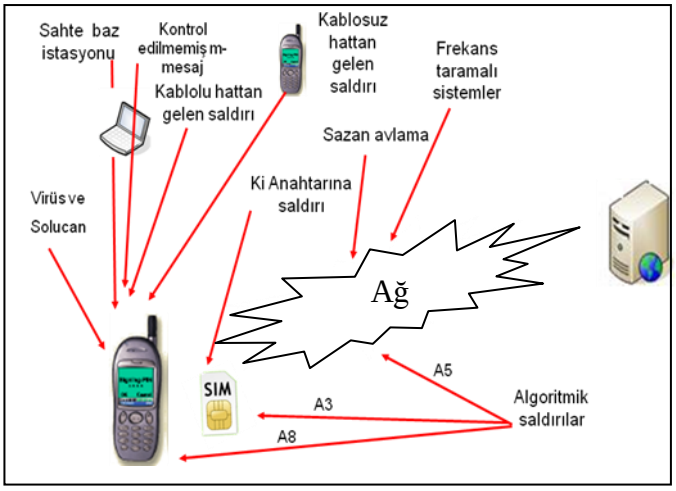
3.9. Algoritmalara yapılan ataklar

Wagner ve Golberg nisan 1998 de COMP128 algoritmasını kırdıklarını açıklamışlardır. Bu algoritma günümüzde pek çok operatörün SIM kartlarında kullandıkları A3/8 bir fonksiyonudur. Bu algoritmada zayıflığın, 160000 seçilmiş RAND-SRES çiftinin elde edilmesiyle bu algoritmanın kolaylıkla kırılabilmesidir [7]. Bunun yanında A5/1 algoritmasına ataklar yapılabileceği ve 2 dakikalı veri toplanmasıyla bu algoritmanın pratik olarak kırılabileceğini göstermiştir [24].

4. Genel Değerlendirmeler

Bu çalışma kapsamında [1]-[24] nolu kaynaklar incelenmiş ve incelenen çalışmalarda meydana gelen açıklar ile GSM şebekelerine yapılabilecek saldırılar Şekil 9'da genel olarak özetlenmiştir.

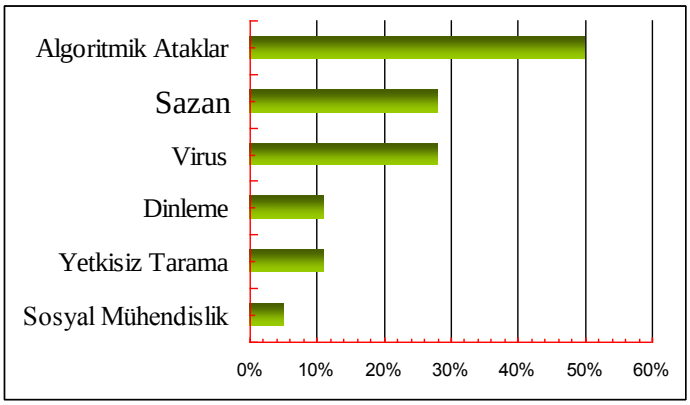
Bu çalışma kapsamında incelenen çalışmalar; algoritmik ataklar, sazan avlama, virüsler, dinleme, yetkisiz tarama ve sosyal mühendislik saldırıları yönünden sınıflandırılmıştır. Bu saldırılarda, algoritmik atakların en fazla olduğu, sazan avlama ve virüsün bunları takip ettiği anlaşılmıştır. Şekil 10'da mobil istasyona yapılan saldırı türleri verilmektedir. Dinleme, yetkisiz tarama ve sosyal mühendislik saldırılarının da bu sistemlere yapıldığını belirlemekte de fayda vardır.



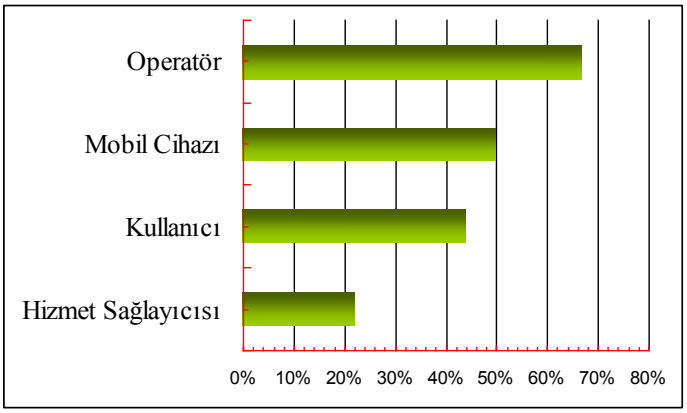
Şekil 9. GSM sistemine yapılan saldırılar

Mobil sistemlere yapılan saldırılar açısından incelenen kaynaklar değerlendirildiğinde, Şekil 11'de elde edilen sonuçlar verilmiştir. Buna göre operatörlere karşı yapılan saldırıların gerçekten çok fazla olduğu ve operatörlerin en zayıf noktalardan biri olduğu görülmüştür. Ancak, Şekil 11'de görüldüğü gibi yapılan araştırmalarda hizmet sağlayıcısı saldırıları hakkında yapılan saldırıların ve araştırmaların daha az olduğu görülmektedir. Bu da hizmet sağlayıcılarının daha güçlü güvenlik sunduklarının göstergesidir. Ancak hizmet sağlayıcısı iletişimde çok önemli bir faktör olduğundan güvenliğin en üst seviyede tutulması gerekmektedir. Şu ana kadar yapılan saldırıların genellikle hizmet sağlayıcılarına karşı yapılmamasından dolayı hizmet sağlayıcılarının güvenlikleri iyi olarak bilinmektedir. Bu bağlamda, önemli olan yerlerin güvenliği devamlı olarak geliştirilmeli ve kontrol edilmelidir.

[14] Uluslararası Mobil Abone Kimlik



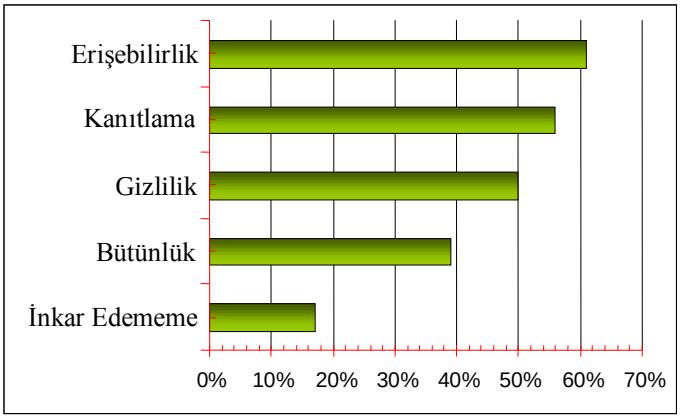
Şekil 10. Mobil sistemine yapılan saldırı türleri



Şekil 11. Mobil sistemine yapılan saldırılar

Şekil 12'de güvenlik bileşenlerinin ihlali hakkında yapılan araştırmalar incelenmiş ve bu kaynaklardan elde edilen sonuçlar yüzde olarak verilmiştir. İnternet ortamında yapılan iletişimlerde en fazla ihlal edilen bileşenler görülmektedir. Burada en fazla güvenlik ihlalinin erişilebilirlik bileşeninde olduğu görülmektedir. İnkar edememe ve bütünlük gibi önemli bileşenlerde yapılan çalışmaların daha az olduğu görülmektedir.

Mobil ortam güvenliği bilgi güvenliği açısından genel olarak değerlendirildiğinde, Şekil 12'de verilen bütün unsurlara aynı miktarda önem vermek gerekmektedir. Bunlardan bir tanesinin ihlali bile güvenliğin ihlaline sebep olmaktadır. Bu kapsamda, bütün unsurlar hakkında daha fazla araştırma ve çalışma yapılması sistemin daha güvenli hale gelmesi için uygun bir adım olabilir.



Şekil 12. Güvenlik bileşenlerinin ihlali

Son günlerde ülkemizde mobil ortamlarda daha güvenli hizmet verilmesine yönelik olarak sunulan çözümler incelendiğinde, mobil elektronik imzanın bunların başında geldiği ve bunun tüm dünyaya örnek olabilecek bir çözüm olduğu ve dünyaya da sunulduğu bilinmektedir. Bununda ülkemiz adına gurur verici olduğunu belirtmekte fayda vardır.

Teknolojik gelişmeler arttıkça doğal olarak bunların günlük hayatımızda kullanımı artacak, istenmeyen durumlarla, oluşabilecek ihlallerle veya saldırılarla her zaman karşılaşılabilecektir. Bu ihlal ve saldırılardan korunmak ve güvenliği sağlamak için bu konularda daha fazla araştırma yapılması, yapılan araştırmaların yayınlanması, teknolojileri güvenli kullanma konusunda kullanıcılar da bilgi sahibi olmalıdırlar.

5. Sonuç ve öneriler

Son günlerde mobil elektronik ortamların kullanımı yaygınlaştıkça bu ortamlardaki güvenlik veya bu ortamlara güven önemli halegelmiştir. Bu çalışmada mobil elektronik ortamlarda meydana gelebilecek güvenlik açıklıkları literatürdeki çalışmalar gözden geçirilerek değerlendirilmiştir. Elde edilen sonuçlar, mobil elektronik ortamlarda verilen hizmetlerde farklı güvenlik açıkları oluşabileceği, bu ortamlarda oluşan açıkların veya tehditlerin çoğunun kullanıcı zafiyetlerinden kaynaklandığı belirlenmiştir. Mobil elektronik ortamların güvenlik seviyelerinin yükseltilmesinin güncel olarak oluşan teknik zafiyetlerinde ortadan kaldırılmasıyla sağlanabileceği unutulmamalıdır.

Teknik olarak yapılacak işlemlerde, me-imza kullanımının farklı açıkları gidermede etkili olacağı ayrıca değerlendirilmektedir. Ülkelerin kullandığı me-imza modelleri incelendiğinde ülkemizde kullanılan modelin en yüksek ve güvenli modeller arasında olduğunu belirlemekte fayda vardır. Mobil ortamlarda meydana gelebilecek bir çok açığın olması sebebiyle her zaman bu ortamlarda yapılabilecek iş ve işlemlerde daha dikkatli olmaları ve bağımsız kuruluşlar tarafından bu ortamlara sızma tesislerinin yapılması pek çok açığın önceden tespit edilmesine fayda vardır.

Son olarak, kullanımı gittikçe artan ve yaygınlaşan mobil ortamları kullanımının hayatımıza daha çok etkinleşip ve bu ortamlarda iş ve işlemleri daha çok yapılmasını kaçınılmaz bir gerçektir. Bu ortamlarda karşılaşılabilecek tehdit ve tehlikeler ile oluşabilecek güvenlik açıklarının giderilmesinde kullanıcıların sorumluluğunun her zaman farkında olmaları hem kullanıcıların daha güvenli ortamlarda haberleşmelerini sağlayacaktır.

Kaynaklar

[1] J. Arreymbi, Modelling to Enhance GSM Network Security, University of East London, Essex, http://ww1.ucmss.com/books/LFS/CSREA2006/SAM5086.pdf
[2] R. Bamforth, B. Tarzey, Mobile Security and Responsibility, Quocirca Insight Report January 2006.
[3] P. Topark-Ngarm, P. Poocharoen, GSM security Vulnerability, http://islab.oregonstate.edu/koc/ece478 /03Report/toparkngarm-poocharoen-project578.pdf.
[4] V. Bocan, V. Cretu, Threats and Countermeasures in GSM Networks, Journal Of Networks, Vol. 1, No. 6, pp: 18-27, November/December 2006.
[5] Y. Li, Y. Chen, T. J. Ma, Security in GSM, http://www.gsm-security.net/papers/securityingsm.pdf.
[6] M. Stausholm, M. Dahl, Insecurity of GSM Communication, Exam project in Cryptography course, DAIMI AU, 2006 December 2006.
[7] P. S. Pagliusi, A Contemporary Foreword on GSM Security, Lecture Notes In Computer Science, ISBN:3-540-44309-6, Vol. 2437, Proceedings of the International Conference on Infrastructure Security, pp: 129 – 144, 2002.
[8] Taxonomy of Current and Potential Mobile Threats, 2001-2007 Cloudmark, Inc., January 2007, http://www.cloudmark.com/releases/docs/wp_taxonomy_of_mobile_threats.pdf .
[9] D. E. Castle, A. Darensburg, B. Griffin, T. Hickman, S. P. Warders, and G. A. Jacoby, Gibraltar: A Mobile Host-Based Intrusion Protection System, National Conference on Undergraduate Research, April 2006.
[10] M. Suominen, GSM security, Helsinki University of Technology, 2003, www.netlab.hut.fi/opetus/s38153/k2003/Lectures/g42GSM_security.pdf.
[11] C. X Guo, H. J. Wang and W. W. Zhu, Smart-phone Attacks and Defenses, in Proc. ACM SIGCOMM HotNets 2004, pp. 125-130.
[12] C. Tang, Summary Of Mobile Threats For Year 2005, 2006, www.it-observer.com/pdf/dl/mobile_threat_sum.pdf
[13] V. Bacon, Security and Denial of Service Threats in GSM Networks, Vol.49 (63), 2004, ISSN 1224-600X.

[14] A. Ahmad, R. Chandler, A. A. Dharmadhikari, and U. Sengupta. SIM-Based WLAN Authentication for Open Platforms. Technology at Intel Magazine, August 2003.
[15] E. Çetintaş, A. Levi, M. Aydos, Ç.K. Koç and M.U. Çağlayan, "Relay Attacks on Bluetooth Authentication and Solutions", LNCS 3280, ISCIS 2004, Antalya, October 2004.
[16] E. Bonesa, P. Hasvolda, E. Henriksena, T. Strandenæsb, Risk analysis of information security in a mobile instant messaging and presence system for healthcare, international journal of medical informatics, IJB-2286, pp.11, 2006.
[17] M. Morioka, Y. Yonemoto, T. Suzuki, M. Etoh. Scalable Security Description Framework for Mobile Web Services, Communications, 2003. ICC '03. IEEE International Conference on Publication, 11-15 May 2003, pp: 804- 808, Vol.2, ISBN: 0-7803-7802-4
[18] E. Barkan, E. Biham, N. Keller, Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication, 2003, http://cryptome.org/gsm-crack-bbk.pdf
[19] M. A. Mohammed Amin, "Mobil Elektronik İmza", **Yüksek Lisans Tezi**, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara 2007.
[20] In-Stat, "3g cellular deployment report," http://www.instat.com, March, 2006.
[21] A. Bose and K. G. Shin, On Mobile Viruses Exploiting Messaging and Bluetooth Services, **Securecomm and Workshops, 2006** Aug. 28-Sept. 1 2006, pp.1-10, ISBN: 1-4244-0423-1.
[22] P. Howard, .GSM and 3G Security., lecture notes, Royal Holloway, University of London, 19 Nov 2001, http://www.isg.rhbnc.ac.uk/msc/teaching/is3/is3.shtml.
[23] M. Walker and T. Wright, Security, in F. Hillebrand, Editor, *GSM and UMTS: The Creation of Global Mobile Communication*, pp. 385-406, John Wiley & Sons, New York, 2002.
[24] A. Biryukov, A. Shamir, D. Wagner, Real time cryptanalysis of A5/1 on a PC., in *FSE 2000*, LNCS No. 1978, Springer Verlag, Berlin, 2000